

UNITED STATES DISTRICT COURT

for the
District of MaineDISTRICT COURT
BANGOR, MAINE
RECEIVED AND FILED

2016 DEC -9 P 1:12

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Information associated with Yahoo! account
JRELS2@YAHOO.COM (Attachment A)

Case No. 1:16-mj-00257-JCN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
Information associated with Yahoo! account JRELS2@YAHOO.COM that is stored at premises owned, maintained, controlled, or operated by Yahoo!, Inc., a company headquartered in Sunnyvale, California (Attachment A)

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 2252A(a)(5)(B), 2252A(a)(2) and 2252(a)(2)	Possession of Child Pornography and Receipt of Child Pornography

The application is based on these facts:

Affidavit of Gregory M. Kelly, Special Agent, HSI

- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Gregory M. Kelly, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/09/2016

City and state: Bangor, Maine

Judge's signature

John C. Nivison, US Magistrate Judge

Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Yahoo! account **JRELS2@YAHOO.COM** that is stored at premises owned, maintained, controlled, or operated by Yahoo!, Inc. a company headquartered in Sunnyvale, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Yahoo!, Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 4, 2016, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. Any and all information for any subscriber(s) associated with account, but not limited to, all subscriber information, such as name and address, date of birth, gender, telephone numbers, screen names/nicknames/identities, date account created, account status, email address, alternate email address, registration from IP address, date ID registered, account history, subscriber complaints and communications with Yahoo!, log-in IP addresses associated with session times and dates and listing of Yahoo! properties used.
- b. For the subscriber(s) identified in Paragraph A above, the contents of any and all emails and email communications stored in the subscriber’s Yahoo! account, including, but not limited to, header information for each item of mail, for the period of June 16, 2012 through September 26, 2012;
- c. For subscriber(s) identified in Paragraph A above, the contents of any and all electronic files (including but not limited to images and videos) that the

subscriber(s) has stored in any areas/properties associated with such Yahoo! accounts for the period of June 16, 2012 through September 26, 2012;

- d. For the subscriber(s) identified in Paragraph A above, any and all other content associated with the account, including but not limited to, images, videos, and electronic files for the period of June 16, 2012 through September 26, 2012;
- e. For the subscriber(s) identified in Paragraph A above, any and all billing records or methods of payment provided by the subscriber to Yahoo! for any services;
- f. For the subscriber(s) identified in Paragraph A above, all records of subscriber account preferences including but not limited to the name and Internet address of any "favorite places" bookmarked web sites, address books, "buddy lists", subscriber profiles, and subscriber privacy and account preferences, and;
- h. For the subscriber(s) identified in Paragraph A above, any location services data retained by Yahoo!.
- i. For all the information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider shall disclose responsive data, if any, by sending to Homeland Security Investigations, 324 Harlow Street, Bangor, Maine 04401 using the US Postal Service or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of **18 U.S.C. 2252A(a)(2) and (a)(5)(B)**, those violations involving the user(s) of the account and occurring between June 16, 2012 and September 26, 2012, including, for each account identified in Attachment A, information pertaining to the following matters:

- a. Receipt, possession, or access with intent to view child pornography, or records pertaining to an interest in child pornography;
- b. Evidence indicating how and when the email account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the email account owner;
- c. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- d. Records relating to the identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- e. Records relating to the identity of the person(s) who communicated with the user ID concerning the identity and location of the account user, an interest in child pornography, or the trading in child pornography, including records that help reveal the whereabouts or any such person(s).

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
JRELS2@YAHOO.COM THAT IS STORED
AT PREMISES CONTROLLED BY
YAHOO!, INC.

Case No. 1:16-mj-257-JCN

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Gregory M. Kelly, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the Yahoo! user account, identified as jrels2@yahoo.com, where the information associated with this account is stored at premises owned, maintained, controlled, or operated by Yahoo! Inc., headquartered at 701 First Avenue, Sunnyvale, California 94089. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Yahoo, Inc. to disclose to the government copies of information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent (SA) with Homeland Security Investigations (HSI), and have been since 2007. Since approximately May 2010, I have been assigned to conduct investigations of crimes where computers and the Internet are used in the sexual exploitation of children, including (but not limited to) violations of 18 U.S.C. Sections 2252 and 2252A, which

prohibit a person from knowingly transporting, receiving, distributing, possessing or accessing with intent to view, in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, child pornography, as defined in 18 U.S.C. Section 2256(8). I have received formal and on-the-job training in the investigation of cases involving the sexual exploitation of children. My experience includes participation in the execution of numerous search warrants involving child pornography and seizures of computers and other storage media, and I have participated in numerous arrests and interviews of subjects involved with child pornography and child exploitation.

3. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

4. The facts set forth in this affidavit are based on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2252A(a)(5)(B), possession of child pornography, and 2252A(a)(2) and 2252(a)(2), receipt of child pornography have been committed by the user of the jrels2@yahoo.com account. There is also probable cause to search the information described in Attachment A for evidence related to these crimes, as described in Attachment B.

BACKGROUND OF THE INVESTIGATION

6. Since October 2012, the U.S. Immigration and Customs Enforcement's (ICE), Homeland Security Investigations (HSI), New York Field Office, Child Exploitation Group (CEG) and Computer Forensics Unit (CFU), have been assisting the Ontario Provincial Police (OPP) and the Toronto Police Service (TPS) in investigating a website that has been used extensively by persons interested in exchanging images depicting child pornography. For purposes of this affidavit, and in order to protect other ongoing investigations, the website is being referred to as "Website A". The following is a description of how Website A operated in October 2012.

7. Website A was a file sharing website hosted outside of the United States. Website A provided both a basic "Free" access and a paid "Premium" tier. Users on the basic tier were unable to access some content and would experience significantly slower download speeds. Website A included no search function, forums, or community of any kind. Links were often shared on websites such as pastebin.com or via E-mail. In addition, Website A included no description, other than the file name itself, or preview of the file. The description, file name or preview that generated the user's interest in the file, therefore, would come from the referring site or the individual providing the link.

8. Users of the Website A file hosting service appear to have had above-average technical ability and in most cases took substantial steps to obfuscate the contents of the files they uploaded for distribution. They accomplished this through the use of compressed files which were password protected and sometimes contained several levels of additional password protected compressed archive file containers, which in turn contained large volumes of images.

9. The investigation revealed that Website A became a popular means for individuals to trade child pornography images and videos.

10. There were two ways to register an account, and thus become a “member” of Website A. The first way to register an account with Website A was for the user to provide their own username, password and email address. The second way to register an account with Website A was to “quick register” in which the user’s username and password was auto-generated by the system and emailed to the user. Once a user signed up to become a member of Website A, the user received a registration confirmation email from Website A. Once accomplished, the user, as a member, could download or upload images and/or videos. Once a member uploaded a file, Website A provided the user with a link that the user could share with others.

11. In approximately October 2012, OPP and TPS obtained a portion of Website A data, including information related to Website A usernames, email addresses, server logs, and stored content. This information was obtained by OPP and TPS as a direct result of a Canadian criminal code search warrant. HSI subsequently received a subset of this information as part of the joint investigation. Due to the volume of information seized by OPP and TPS from 32 servers leased to Website A, there was a delay in processing the information. There were approximately 60,000 individuals registered as users of Website A at the time of the seizure and the total number of RAR archive files associated with those users was approximately 1.4 million. A RAR file can be described as a compressed file container which can hold multiple additional files in similar fashion to a “Russian doll” and can be encrypted/password protected. When the RAR file is extracted or uncompressed, it can contain several hundred or even thousands of images and/or videos. Additionally, the total size of data seized from the Website A servers was

approximately 1,500 terabytes. A one terabyte hard drive will hold approximately 500,000 images or about 1,000 hours of digital movies.

DETAILS OF THE CURRENT INVESTIGATION

12. After reviewing the Website A data, investigators identified the screenname “CRASS” as a member of Website A who had downloaded child pornography. At the time of the download, Website A logged CRASS’ Internet Protocol (IP) address as 74.75.74.40 which investigators later learned geo-located to the Fairfield, Maine area. The CRASS lead was eventually forwarded to HSI New York before it was subsequently forwarded to HSI Bangor, Maine in September 2016. I reviewed the lead materials and learned that on June 16, 2012, an individual created an account on Website A and assigned him or herself the username CRASS. CRASS associated an email address of jrels2@yahoo.com with the Website A account. On or about June 22, 2012, CRASS downloaded a RAR file, identified as ‘picc.rar’, containing approximately 96 image files from Website A. I reviewed the content of these files and determined the majority to depict prepubescent female children engaged in sexually explicit conduct and/or a lascivious display of their genitals. Three of the images downloaded by CRASS are described as follows:

- a) The image file “IMG_2145.JPG” depicts a naked prepubescent female lying on her back. There is a naked adult male standing between the prepubescent female’s spread legs and his erect penis is penetrating the female’s vagina.

(attached under seal as exhibit 1)

- b) The image file “IMG_2146.JPG” also depicts a naked prepubescent female lying on her back. There is a naked adult male standing between the prepubescent

female's spread legs and his erect penis is penetrating the female's vagina.

(attached under seal as exhibit 2)

- c) The image file "IMG_2155.JPG" depicts two naked prepubescent females. One child is lying on her back with her legs spread apart. The other child is lying on her stomach between the other child's legs and appears to be licking the child's vulva. **(attached under seal as exhibit 3)**

13. In addition to the RAR file containing child pornography, I noted two additional files downloaded from Website A by CRASS which occurred in September 2012 using the same IP address as noted above. Both files had names indicative of software programs with the first entitled, "Video Copilot – Sound & Music Pack (objfbx).rar" and the second entitled, "Poser_Pro_2012_SR3_Update_for-Windows.rar". I was not provided any information concerning the contents of these files. I was also not provided any records of CRASS downloading additional files from Website A other than the three noted above. The download of the two files in September are evidence that CRASS continued to use Website A after downloading child pornography in June 2012. I do not believe that if someone had inadvertently downloaded child pornography from Website A that they would continue to use Website A to download files. I believe most users would discontinue use of such a website. I believe CRASS' continued use of Website A after downloading the 'picc.rar' file containing child pornography indicates that CRASS did not inadvertently download child pornography.

14. After fully reviewing the lead materials, I noted that there was no data identifying the user of the CRASS account other than the IP address logged by Website A in 2012. No IP subscriber information was obtained at that time that would have identified the subscriber to the IP address. I know through experience that most Internet Service Providers will only retain IP

subscriber information for approximately 6 months. Therefore, I am currently unable to identify the subscriber to the IP address on the date and time CRASS downloaded child pornography from Website A.

BACKGROUND CONCERNING EMAIL

15. In my training and experience, I have learned that Yahoo! provides a variety of on-line services, including electronic mail ("email") access, to the public. Yahoo! allows subscribers to obtain email accounts at the domain name yahoo.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Yahoo!. During the registration process, Yahoo! asks subscribers to provide basic personal information. Therefore, the computers of Yahoo! are likely to contain stored electronic communications (including retrieved and unretrieved email for Yahoo! subscribers) and information concerning subscribers and their use of Yahoo! services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user.

16. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit card or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my

experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

17. A Yahoo! subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Yahoo!. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

18. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

19. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems or billing inquiries. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the

crimes under investigation because the information can be used to identify the account's user or users.

20. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Lastly, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or

consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

21. On October 4, 2016, I submitted a preservation request for this account to Yahoo! Inc. In general, an email that is sent to a Yahoo! subscriber is stored in the subscriber's "mail box" on Yahoo! servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Yahoo! servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Yahoo! servers for a certain period of time.

22. Therefore, the computers of Yahoo! are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Yahoo!, such as account access information, transaction information, and other account information.

INFORMATION CONCERNING CHILD EXPLOITATION INVESTIGATIONS

23. Based upon my knowledge and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

- a. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification.

- b. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- c. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. They often maintain these collections for several years and keep them close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.
- d. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; they rarely destroy correspondence from other child pornography distributors/collectors; they conceal such correspondence as they do their sexually explicit material; and they often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

24. I have probable cause to believe and I do believe that the content of, and the records associated with, the jrels2@yahoo.com account will provide evidence of the identity of

CRASS. I know from the information provided by HSI New York that upon creating an account on Website A, the user received a registration confirmation email at the email address they associated with their account. In this case, CRASS would have received a registration confirmation email from Website A at jrels2@yahoo.com. This email will confirm that CRASS created the Website A account and could provide information that would help identify CRASS. As noted above, I know that collectors of child pornography rarely destroy their correspondence with other child pornography collectors or in this case a website used extensively for the trading of child pornography. I believe it probable that CRASS would retain the registration email for future reference as access to a website known for the trading of child pornography would be very valuable to a child pornography collector.

25. I also believe that CRASS used the jrels2@yahoo.com email address to correspond with other users about child pornography. I know from the information provided to me by HSI New York that CRASS could not search Website A for the child pornography CRASS downloaded as Website A did not support searches. I also know that many of the files on Website A, to include the 'picc.rar' file downloaded by CRASS, did not have file names immediately apparent or indicative of containing child pornography. I believe CRASS learned of and obtained knowledge of the contents of the 'picc.rar' file through email correspondence from other Website A user(s). I believe CRASS corresponded with these user(s) via email as Website A did not contain any forums or other mechanism that would allow Website A users to communicate. As CRASS associated the jrels2@yahoo.com account with his/her Website A account, I believe CRASS used this email address to correspond with other Website A user(s).

26. I also believe that CRASS' additional downloads in September 2012 indicate that CRASS was interested in child pornography. According to the lead materials provided by HSI

New York, CRASS downloaded three files during the period reviewed. The first of the three downloads was a file containing approximately 96 child pornography files. I believe most users would have discontinued usage of a website from which they had downloaded child pornography unless that is the type of file they had wanted. As CRASS continued to use Website A after the initial download of child pornography, this indicates to me that CRASS sought out and intended to download the child pornography that he/she downloaded in the 'picc.rar' file.

27. I believe a review of the email content for the jrels2@yahoo.com account during the period from the creation of the CRASS account on Website A through the date of the last download by CRASS will provide evidence of CRASS' identity. I have identified this period as June 16, 2012 through September 26, 2012. I also believe that a review of the most recent subscriber information and Internet Protocol connection logs for the jrels2@yahoo.com account will provide evidence of CRASS' identity.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

28. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Yahoo! to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

29. Based on the forgoing, I request that the Court issue the proposed search warrant.

30. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

31. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the provider may retrieve this information at a time outside of normal Eastern Standard day-time hours, I believe there is reasonable cause to authorize the execution of this warrant at any time of the day or night.

REQUEST FOR SEALING

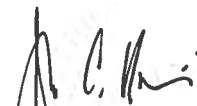
32. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Gregory M. Kelly
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on December 9, 2016



Honorable John C. Nivison
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Yahoo! account **JRELS2@YAHOO.COM** that is stored at premises owned, maintained, controlled, or operated by Yahoo!, Inc. a company headquartered in Sunnyvale, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Yahoo!, Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 4, 2016, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. Any and all information for any subscriber(s) associated with account, but not limited to, all subscriber information, such as name and address, date of birth, gender, telephone numbers, screen names/nicknames/identities, date account created, account status, email address, alternate email address, registration from IP address, date ID registered, account history, subscriber complaints and communications with Yahoo!, log-in IP addresses associated with session times and dates and listing of Yahoo! properties used.
- b. For the subscriber(s) identified in Paragraph A above, the contents of any and all emails and email communications stored in the subscriber’s Yahoo! account, including, but not limited to, header information for each item of mail, for the period of June 16, 2012 through September 26, 2012;
- c. For subscriber(s) identified in Paragraph A above, the contents of any and all electronic files (including but not limited to images and videos) that the

subscriber(s) has stored in any areas/properties associated with such Yahoo! accounts for the period of June 16, 2012 through September 26, 2012;

- d. For the subscriber(s) identified in Paragraph A above, any and all other content associated with the account, including but not limited to, images, videos, and electronic files for the period of June 16, 2012 through September 26, 2012;
- e. For the subscriber(s) identified in Paragraph A above, any and all billing records or methods of payment provided by the subscriber to Yahoo! for any services;
- f. For the subscriber(s) identified in Paragraph A above, all records of subscriber account preferences including but not limited to the name and Internet address of any "favorite places" bookmarked web sites, address books, "buddy lists", subscriber profiles, and subscriber privacy and account preferences, and;
- h. For the subscriber(s) identified in Paragraph A above, any location services data retained by Yahoo!.
- i. For all the information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider shall disclose responsive data, if any, by sending to Homeland Security Investigations, 324 Harlow Street, Bangor, Maine 04401 using the US Postal Service or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of **18 U.S.C. 2252A(a)(2) and (a)(5)(B)**, those violations involving the user(s) of the account and occurring between June 16, 2012 and September 26, 2012, including, for each account identified in Attachment A, information pertaining to the following matters:

- a. Receipt, possession, or access with intent to view child pornography, or records pertaining to an interest in child pornography;
- b. Evidence indicating how and when the email account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the email account owner;
- c. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- d. Records relating to the identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- e. Records relating to the identity of the person(s) who communicated with the user ID concerning the identity and location of the account user, an interest in child pornography, or the trading in child pornography, including records that help reveal the whereabouts or any such person(s).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Yahoo! Inc. and my official title is _____. I am a custodian of records for Yahoo! Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Yahoo! Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Yahoo! Inc.; and

c. such records were made by Yahoo! Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature